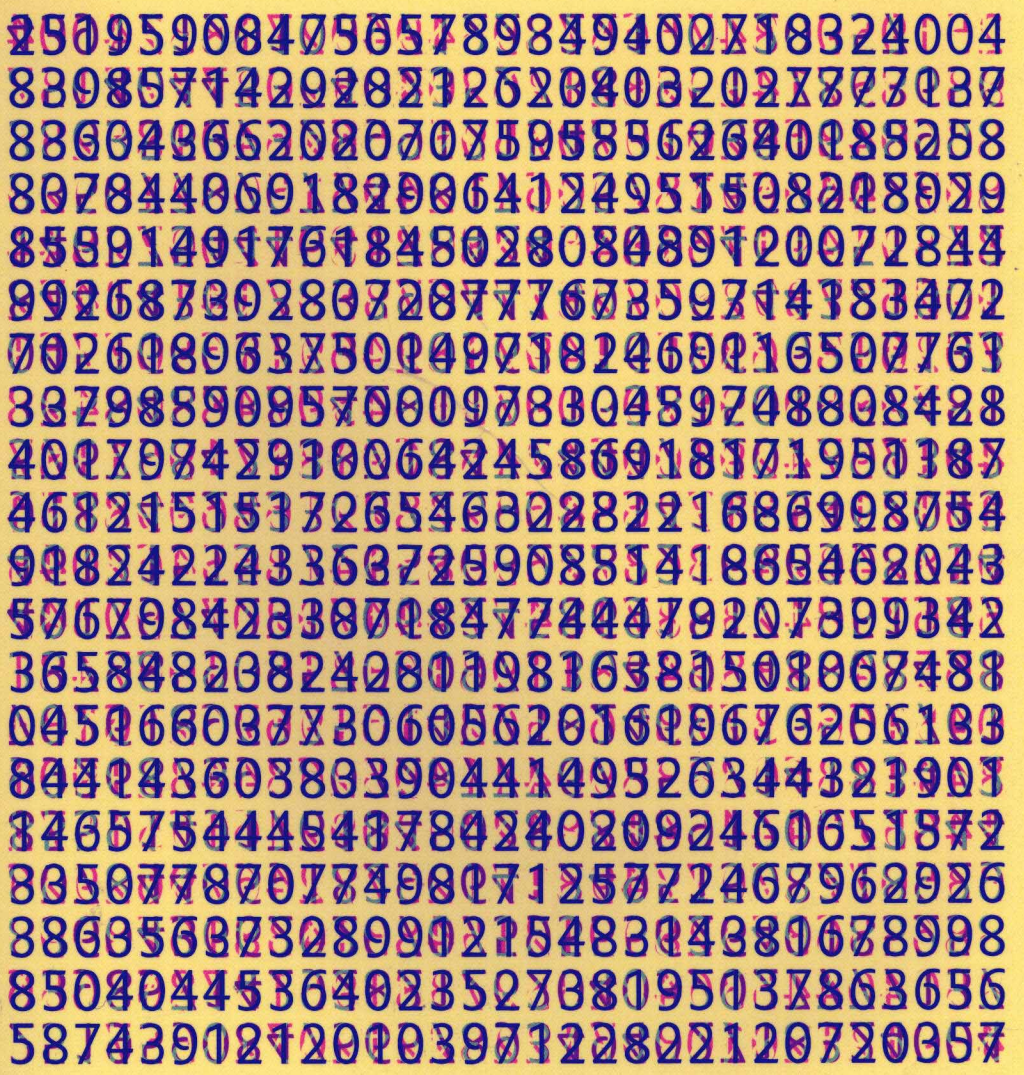
Niels Lauritzen

Concrete Abstract Algebra

From Numbers to Gröbner Bases



CAMBRIDGE

CONCRETE ABSTRACT ALGEBRA

From Numbers to Gröbner Bases

NIELS LAURITZEN
Department of Mathematical Sciences
University of Aarhus
Denmark

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published 2003

Printed in the United Kingdom at the University Press, Cambridge

Typeface Times 9/13 pt. *System* LaTeX 2_ε [TB]

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Lauritzen, Niels, 1964–
Concrete abstract algebra: from numbers to Gröbner bases / Niels Lauritzen.
p. cm.
Includes bibliographical references and index.
ISBN 0 521 82679 9 (hardback) – ISBN 0 521 53410 0 (paperback)
1. Algebra, abstract. 1. Title
QA162.L43 2003
512'.02–dc21 2003051248

ISBN 0 521 82679 9 hardback
ISBN 0 521 53410 0 paperback

CONCRETE ABSTRACT ALGEBRA

From Numbers to Gröbner Bases

Concrete Abstract Algebra develops the theory of abstract algebra from numbers to Gröbner bases, whilst taking in all the usual material of a traditional introductory course. In addition there is a rich supply of topics such as cryptography, factoring algorithms for integers, quadratic residues, finite fields, factoring algorithms for polynomials and systems of non-linear equations. A special feature is that Gröbner bases do not appear as an isolated example. They are fully integrated as a subject that can be taught successfully in an undergraduate context.

Lauritzen's approach to teaching abstract algebra is based on an extensive use of examples, applications and exercises. The basic philosophy is that inspiring, non-trivial, applications and examples give motivation and ease the learning of abstract concepts. This book is built on several years of experience teaching introductory abstract algebra at Aarhus, where the emphasis on concrete examples has improved student performance significantly.

For Helle and William

Preface

Imagine that you have a very persistent piano teacher insisting that you study notes and practice scales for three years before you are allowed to listen to or play any real music. How is that going to affect your level of inspiration? Are you going to attend every lesson with passion or practice absolutely ignited with energy? Abstract algebra is like piano playing. You can kill your inspiration and motivation spending years on formalism before seeing the beauty of the subject. This book is written with the intent that every chapter should contain some real music, matters which involve practice of the notes and scales in a surprising and unexpected way. It is an attempt to include a lot of non-trivial and fun topics in an introductory abstract algebra course. Having inspiring goals makes the learning easier. The topics covered in this book are numbers, groups, rings, polynomials and Gröbner bases.

Knowledge of linear algebra and complex numbers is assumed in some examples. However, most of the text is accessible with only basic mathematical topics such as sets, maps, elementary logic and proofs.

Gröbner bases are usually not treated at an undergraduate level. My feeling four years ago when including this topic in the syllabus at Aarhus was one of hesitation. I was afraid that the material would be too advanced for the students. It turned out that the students liked the concrete nature of the material and enjoyed the non-trivial computations with polynomials. They found it easier than the traditional topics of groups and rings.

Unlike most treatments on Gröbner bases, I have not included any implementations of algorithms in a pseudo-language. My personal experience is that it disturbs the flow of the mathematics when teaching the basic ideas of the algorithms. Once the mathematical concepts and a few examples are understood, it is easy to extract the algorithms for implementation on a computer. In fact

students are very much encouraged to experiment using a computer algebra system especially when learning about numbers and Gröbner bases.

Chapter 1 is on numbers. It is mostly based on the RSA cryptosystem and the mystery that it seems much easier to multiply numbers than to factor them. The 617-digit number on the cover of this book is a product of two prime numbers. If you can find them you should write to RSA Labs and claim the $200,000 prize. Going through the first chapter you will learn basic number theory: division with remainder, congruences, the Euclidean algorithm, the Chinese remainder theorem, prime numbers, how prime numbers uncovered the infamous FDIV bug in Intel's Pentium processor, Fermat's little theorem and how it is used to produce 100-digit prime numbers for the modern information age, three modern algorithms for factoring numbers much faster than by trial division, quadratic residues and the quadratic reciprocity theorem (which will be proved in Chapter 4).

The level of abstraction is increased in Chapter 2. Here the mathematical object is a group. A group is defined using a composition on a set and it satisfies three simple rules. This definition has proved extremely important and invaluable to modern algebra. You get a framework for many proofs and concepts from basic number theory. We treat the basics of group theory, the symmetric and alternating groups, how to solve the 15-puzzle using groups, actions of groups, counting and the Sylow theorems.

In Chapter 3 we treat rings. A ring is an abelian group with multiplication as an added composition. We touch briefly on non-commutative rings, with the quaternions as an example. We then move on to commutative rings, Freshman's Dream, fields, domains, principal ideal domains, Euclidean domains and unique factorization domains. The Fermat two-square theorem (every prime number leaving a remainder of 1 when divided by 4 can be written as a sum of two unique squares (e. g. $13 = 3^2 + 2^2$)) is a prime example in this chapter. You will see the infinitude of prime numbers leaving a remainder of 1 when divided by 4, further use of quadratic residues and an effective algorithm for computing the two squares in the two-square theorem.

Polynomials form a central topic. In Chapter 4 we treat polynomials in one variable. Here the highlights are: cyclotomic polynomials, a proof of the law of quadratic reciprocity using only basic properties of rings of polynomials, how to use floating point arithmetic to compute the order of specific elements in a well known cyclic group, the ElGamal cryptosystem, the infinitude of prime numbers congruent to 1 modulo a natural number > 1 and the existence and uniqueness of finite fields, along with algorithms for factoring polynomials over finite fields.

In Chapter 5 polynomials in several variables and Gröbner bases are treated. Gröbner bases form an exciting and relatively new branch of algebra. They are very concrete and computational. The distance from understanding the abstract concepts involved to computing with them is small. They provide a framework for solving non-linear equations (used in most computer algebra systems) with applications in many areas inside and outside algebra. In Chapter 5 you will see term orders, the fundamental Dickson's lemma, the division algorithm for polynomials in several variables, the existence of Gröbner bases, Hilbert's basis theorem, Buchberger's S-criterion and algorithm, how to write $X^4 + Y^4$ as a polynomial in $X + Y$ and XY (like writing $X^2 + Y^2$ as $(X + Y)^2 - 2XY$) using Gröbner bases and how to solve certain non-linear equations in several variables systematically.

A few exercises are marked **HOF**. This indicates that they are "hall of fame" exercises, far beyond what is required in an introductory abstract algebra course. They usually call for an extraordinary amount of ingenuity. A student capable of solving one of these deserves to be inducted into the hall of fame of creative problem solvers. A hall of fame museum can be suitably maintained using a course home page.

Suggestions for teaching a one-semester course

The book contains too much material for a one-semester course in introductory abstract algebra. So, a selection of material must be made. A possible procedure would be to leave out factoring algorithms from Chapter 1, quadratic reciprocity from Chapters 1 and 4 and the Sylow theorems from Chapter 2. This plan would give a one-semester course ending with Gröbner bases; it would cover the usual topics in an introductory course.

Leaving out Gröbner bases completely, Chapters 1 through 4 would form an in-depth traditional introductory abstract algebra course with many examples.

Acknowledgements

I wish to thank all the students of Algebra 1 at the University of Aarhus during the past four years for carefully listening, asking questions, looking puzzled at the right (or wrong) times and for inspiring me to change my exposition several times. I wish in particular to thank R. Villemoes for many valuable comments and for a set of detailed TEX-solutions to the exercises (available through Cambridge University Press).

Many people influenced this book either by discussions and comments or by patiently answering my numerous questions: T. B. Andersen, H. H. Andersen, M. Bökstedt, J. Brandt, A. Buch, A. L. Christophersen, I. Damgaard, R. Faber Larsen, P. de Place Friis, S. Galatius Smith, W. J. Haboush, J. P. Hansen, G. Hellmund, C. U. Jensen, T. H. Lynderup, T. Høholdt, T. Laframboise, M. Skov Madsen, K. Nielsen, U. Raben Pedersen, M. S. Risager, A. Skovborg, H. G. Spalk, J. Tornehave, H. Vosegaard and A. Venkov.

I am particularly indebted to J. C. Jantzen for reading carefully earlier versions of my Algebra 1 notes. His comments were (as always) extremely relevant and helpful. J. F. Thomsen also read earlier versions of the notes and made detailed comments on the 15-puzzle, which led to substantial improvements. H. A. Salomonsen pointed out a substantial simplification that moved the proof of quadratic reciprocity from the context of finite fields to the more student-friendly environment of the basic theory of polynomials. An anonymous referee from the US made meticulous comments and suggestions which greatly facilitated the process of turning my incomplete notes into the present book. J. Walthoe at Cambridge University Press has been extremely helpful making several insightful suggestions.

This book is for Helle and William. They have unselfishly fueled my writing with their love.

Contents

1 Numbers

This chapter serves as an introduction to the modern theory of algebra through the natural numbers $0, 1, 2, \ldots$. The list of natural numbers never ends and most of them are far beyond everyday use. Gigantic numbers of more than 100 digits are used to protect information transmitted over the internet.

Suppose Alice has to send a message to Bob over the internet and it must be kept secret. Alice and Bob live far apart and many intermediate computers will see the message on its way. Alice will have to scramble (encrypt) the message and send it, but at the same time Bob will have to know how to unscramble (decrypt) it. How does Alice get this information through to him? She could call and tell him. But then again someone could be listening in on their phone call. Is there a way out of this problem?

The answer is an amazing "yes" and it builds on a current paradox of mathematics: the existence of so-called one-way functions $f(X)$. These are functions easy to compute given the input X. Once they are computed and only $f(X)$ is known, it appears to be exceedingly difficult to recover X unless some secret information is known.

Here is an example of a one-way function. Fix a natural number N and let $f(X) = [X^3]$, where $[Y]$ denotes the remainder of Y after division by N. This is a function $f : M \to M$, where $M = \{0, 1, 2, \ldots, N-1\}$. When $N = 15$, f can be tabulated as

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$f(X)$	0	1	8	12	4	5	6	13	2	9	10	11	3	7	14

Of course we can easily find X given $f(X)$ by using the above table. But in general, as N grows the difficulty of finding X given $f(X)$ seems insurmountable unless you know some secret information. In the above example the secret information is that $f(f(X)) = X$ (you can see this using the table). In a sense we are raising a number to the third power and then scrambling things up by

taking the remainder. So far nobody has found effective methods for finding cube roots in this setting. In the above example Alice sends the encrypted message $f(X)$ to Bob and Bob decrypts it using f. This is the basic principle behind the RSA cryptosystem [22], which was the first cryptosystem based on the groundbreaking idea [8] of using one-way functions (with a trapdoor).

On a more detailed level Bob computes two gigantic prime numbers (usually 100 digits or more) p and q and forms $N = pq$. He then uses p and q to compute a number e (for encryption) and a number d (for decryption). He makes the numbers N and e public so that people wishing to write secret messages to him can use the function $f(X) = [X^e]$ for encryption, where $[Y]$ denotes the remainder of Y after division by N. He keeps the function $g(X) = [X^d]$ secret (the point being that $g(f(X)) = X$). In the example above we have $p = 3, q = 5, N = 15, e = 3, d = 3$. One way of systematically finding the secret decryption function g in the RSA system is to find the prime factors p and q of N (N being available to the general public). The straightforward method of trial division (dividing with successive primes $2, 3, 5, \ldots$) is much too slow. Mathematicians have tried at least since Gauss's time (1777–1855) to find faster methods for factoring numbers. In fact Gauss writes in ([11], Art. 329)

> The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i.e., for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator. And these methods do not apply at all to larger numbers.

RSA Labs has put forward several factoring challenges. The hardest unsolved challenge is called RSA-2048. This is the 2048-bit number (617 digits) N on the cover of this book. It is known to be the product of two prime numbers p and q. A computer was instructed to forget p and q after forming $N = pq$. Given two candidates p' and q', it is easy to multiply them to see if their product equals N. This can be done in a small fraction of a second on any modern computer. Nevertheless, finding p and q knowing only N seems to be a painstakingly slow process not within the limits of modern computers and algorithms. If you can find p and q you will be able to claim the $200 000 prize by submitting your factorization via http://www.rsasecurity.com/go/factorization.html. Alternatively, you could settle for the less ambitious RSA factoring challenges presented at

http://www.rsasecurity.com/rsalabs/challenges/factoring/numbers.html. It has not been proved mathematically that factoring a number is a difficult problem in a precise sense, so a fast algorithm may exist waiting to be discovered. In a sense this would disrupt the pillars of the modern information age. The algebraic reasoning behind the RSA cryptosystem is founded on basic results (more than 300 years old) about the natural numbers.

1.1 The natural numbers and the integers

The natural numbers $1, 2, 3, \ldots$ were handed over to mankind by God (in the words of Kronecker (1823–91)). Mankind later added the important natural number 0. We will reserve the symbol $\mathbb{N}$ for the natural numbers $\{0, 1, 2, 3, \ldots\}$. The need for negative numbers leads us to introduce the set of integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ containing the natural numbers $\mathbb{N}$. We have deliberately cut through the red tape of formally defining $\mathbb{N}$ and $\mathbb{Z}$ here. We will also take the addition (and subtraction) and multiplication of integers for granted. This will be the starting point of our study of numbers.

1.1.1 Well ordering and mathematical induction

For $X, Y \in \mathbb{Z}$ we define $X \leq Y$ if $Y - X \in \mathbb{N}$ and $X < Y$ if $X \neq Y$ and $X \leq Y$. This leads to the usual way of ordering the integers,

$$\cdots < -3 < -2 < -1 < 0 < 1 < 2 < 3 < \cdots .$$

An element s in a subset $S \subseteq \mathbb{Z}$ is said to be a first element in S if $s \leq x$ for every $x \in S$. There are many subsets of $\mathbb{Z}$ that do not have a first element. If a subset of $\mathbb{Z}$ has a first element then the latter has to be unique (see Exercise 1.1 at the end of the chapter). The basic axiom for starting our investigation of numbers says that *every non-empty subset of* $\mathbb{N}$ *has a first element.* We also say that the set of natural numbers is *well ordered.*

The property that $\mathbb{N}$ is well ordered is equivalent to mathematical induction. Recall that mathematical induction says that if we are given statements $P(n)$ for every integer $n \geq 1$ such that

(i) $P(1)$ is true and
(ii) $P(n)$ is true implies that $P(n + 1)$ is true

then $P(n)$ is true for every $n \geq 1$.

Example 1.1.1 Let us prove the formula

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \tag{1.1}$$

for $n \in \mathbb{N}$ using mathematical induction. This means that we consider (1.1) as a statement $P(n)$. Clearly $P(1)$ is true, since $1 \cdot (1+1) = 2$. Suppose now that $P(n)$ is true. Then

$$1 + 2 + \cdots + n + (n+1) = \frac{n(n+1)}{2} + (n+1).$$

The right hand side can be rewritten as

$$\begin{aligned} \frac{n(n+1)}{2} + (n+1) &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

This is the formula for $n+1$. So we have proved that $P(n)$ implies $P(n+1)$. By mathematical induction we have proved $P(n)$ for every $n \geq 1$.

Of course, having the formal machinery for constructing a proof like this does not necessarily provide the beauty of a really ingenious mathematical argument. When Gauss was in school (at the age of seven) his mathematics teacher asked the class to sum up all numbers from 1 to 100. The students worked furiously with their small slates. Gauss was the first to give his slate with the number 5050 to the teacher. The teacher replied "Oh, I see, you probably knew the answer." "No, no! I just realized that

$$\begin{aligned} 1 + 100 &= 101, \\ 2 + 99 &= 101, \\ 3 + 98 &= 101, \\ &\vdots \\ 100 + 1 &= 101. \end{aligned}$$

Therefore $1 + 2 + \cdots + 100 = (100 \cdot 101)/2 = 5050$," Gauss replied.

1.2 Division with remainder

Suppose that you mark all multiples of 3 on the axis of the integers: